Log File Analyzer for Intrusion Detection

Introduction

During my internship, I worked on building a Log File Analyzer for Intrusion Detection. The idea was to understand how logs can be used in cybersecurity to detect attacks. By parsing and analyzing log files, I was able to create reports and charts that clearly show attack patterns. This project helped me get hands-on experience in both Python programming and cybersecurity concepts like brute-force detection, scanning, and DoS.

Abstract

This project is about analyzing Apache and SSH logs to detect suspicious activities like brute-force login attempts, port scanning, and possible DoS attacks. The tool is built in Python and generates structured reports (CSV, TXT, PDF) along with visualizations (charts and graphs). The main goal was to create a simple log analyzer for cybersecurity learning and practice.

Tools & Technologies Used

Python – programming language used
Pandas – for handling and analyzing log data
Matplotlib & Seaborn – for creating visualizations
Regex – to match patterns in logs
ReportLab – for PDF report generation
Pytest – for testing modules

Steps Taken (Work Summary)

1. Created project structure and setup environment.
2. Parsed Apache and SSH logs using regex and Python.
3. Implemented modules to detect:
   Brute-force attempts
   Port scanning
   DoS attacks
4. Generated reports in CSV, TXT, PDF formats.
5. Created visualizations like top IPs, failed login attempts, request trends.
6. Added blacklist checking for suspicious IPs.
7. Optimized code by adding comments and modular functions.
8. Collected screenshots of reports, charts, and logs for documentation.
9. Tested tool end-to-end with multiple sample logs.

10. Cleaned GitHub repo and finalized documentation.

Results & Analysis

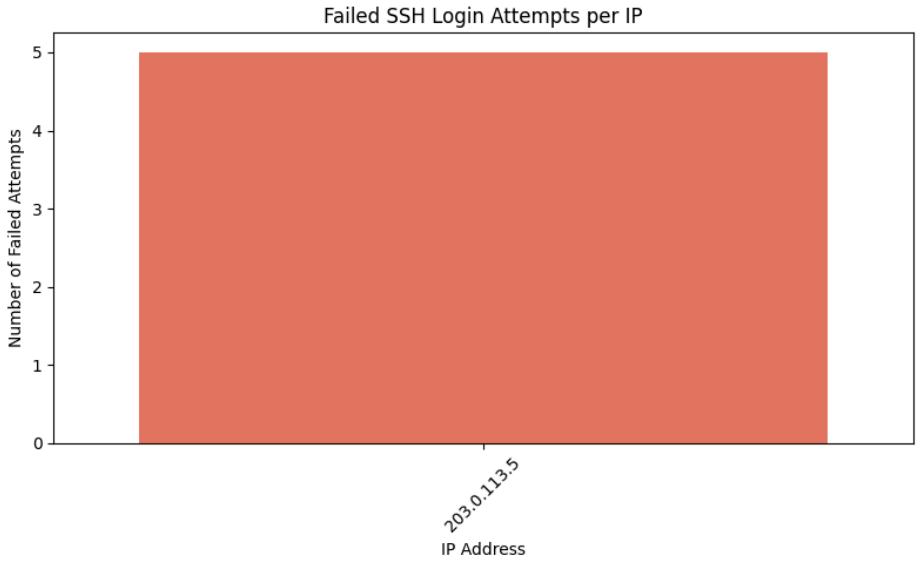

Figure 1: Failed login attempts per IP from SSH logs.

Final Report Output

Incident Report

2025-08-29 14:32 - Failed login from 192.168.1.10
2025-08-29 15:10 - Port scan from 203.0.113.45

Figure 2: Generated incident report summarizing suspicious activities.

Conclusion

This project gave me practical exposure to SOC and DFIR skills. I learned how logs play an important role in detecting attacks and how automation can save time in analysis. The project also improved my coding, debugging, and documentation skills. Overall, it was a good experience and a useful step towards my cybersecurity career.